Multimed Tools Appl (2018) 77:17853–17859
https://doi.org/10.1007/s11042-018-5831-x

GUEST EDITORIAL

Guest Editorial: Multimedia Information Security and Its Applications in Cloud Computing

Chuan Qin [1] · **Weiming Zhang** [2] · **Xinpeng Zhang** [3]

Published online: 3 April 2018

Multimedia applications are omnipresent in our daily lives, however, a lot of relevant security issues have emerged as well, such as covert communication using multimedia files, copy-move forgery in digital images and videos, and biometric spoofing. To address these issues, many multimedia information security techniques were proposed by utilizing the methods in areas like machine learning, signal and image processing, and communications. Nevertheless, there still exist some obvious shortcomings in the research methodologies. Current multimedia security studies are often based on the strict conditions that are nearly impossible to meet up in real world. Furthermore, high computational complexity of current methods makes it hard to handle the big data in the environment of cloud computing. All these drawbacks limit the applications of the forensics and other secure techniques in practice, which deserve the in-depth investigations.

This special issue aims to bring together the latest research works in the related fields of multimedia information security, which emphasizes on the novel and efficient methodologies that have the potentials to be applied in secure cloud computing. According to the rigorous review procedure consisting of several rounds, each of the 34 manuscripts submitted to the special issue was technically reviewed by at least three anonymous experts. Finally, 18 papers are selected to be included in this special issue, which fall into five main categories: (1) *steganography* (4 papers), (2) *steganalysis* (5 papers), (3)

✉ Chuan Qin
qin@usst.edu.cn

Weiming Zhang
zhangwm@ustc.edu.cn

Xinpeng Zhang
zhangxinpeng@fudan.edu.cn

[1] School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

[2] School of Information Science and Technology, University of Science and Technology of China, Hefei 230026, China

[3] School of Computer Science, Fudan University, Shanghai 200433, China

reversible data hiding (4 papers), (4) *Cryptography* (2 papers), and (5) *other emerging techniques* (3 papers). In the following, we introduce these papers briefly.

1 Steganography

The paper titled "Which Gray Level Should be Given the Smallest Cost for Adaptive Steganography?" (https://doi.org/10.1007/s11042-017-4565-5), co-authored by Yao Wei, Weiming Zhang, Weihai Li, Nenghai Yu, and Xi Sun, exploits the relationship between change costs of steganography and gray level in spatial domain via Gamma encoding. In their proposed scheme, the gray level that changes most greatly after the Gamma encoding is assigned with the smallest cost. The cost of each pixel is only linked to its gray level and independent with its position. Experimental results show that, compared with the prior position dependent schemes, the proposed scheme has lower time complexity and can be applicable for the situation with higher speed requirements. In spite of security deficiency, this scheme reveals an interesting relationship between steganographic costs and gray levels.

"Distortion Function based on Residual Blocks for JPEG Steganography" (https://doi.org/10.1007/s11042-017-5053-7) is presented by Qingde Wei, Zhaoxia Yin, Zichi Wang, and Xinpeng Zhang. The authors propose a distortion function for JPEG steganography based on residual blocks, in which residual block values (RBV) and quantization steps are involved to obtain less statistical detectability. Detailedly, the RBVs and the quantization steps are used to determine the embedding risk caused by DCT block modifications and of selection channel, respectively. With the help of syndrome trellis coding (STC), the secret data can be embedded and modifications are restricted in hard-to-detect regions. Experiments show that, the proposed method performs better than some of state-of-the-art methods for JPEG steganography.

Common steganographic schemes aim to embed the fixed-length secret message into the cover while minimizing the distortion to the stego. However, in some applications, the sender requires to embed a variable-length secret payload with expected stego security, which is called as the problem of secure payload estimation (SPE). In the paper "A Priori Knowledge Based Secure Payload Estimation" (https://doi.org/10.1007/s11042-017-4955-8), Sai Ma, Xianfeng Zhao, Qingxiao Guan, Zhoujun Xu, and Yi Ma focus on solving the SPE problem based on two priori knowledge functions, which reflect the relationship between detection error rate and stego distortion and the relationship between stego distortion and payload rate, respectively. Although there exists the coding loss in the results, the proposed method can still be considered as a valuable practical approach for capacity estimation.

In another paper titled "Dither Modulation Based Adaptive Steganography Resisting JPEG Compression and Statistic Detection" (https://doi.org/10.1007/s11042-017-4506-3), Yi Zhang, Xiaodong Zhu, Chuan Qin, Chunfang Yang, and Xiangyang Luo propose an adaptive steganography algorithm, which can resist JPEG compression and detection, by using the dither modulation technique. According to adaptive dither modulation algorithm based on quantization tables, the embedding domains resisting JPEG compression for spatial and JPEG images are individually determined. With the embedding costs calculation based on side information, the embedding cost function can be constructed and the RS coding is combined with STCs to achieve the minimum cost caused by embedding and the improved accuracy of extracted data after JPEG compression. Experimental results demonstrate that, the proposed algorithm not only has the JPEG resistant ability, but also possesses a strong detection resistant performance.

2 Steganalysis

The paper titled "Markov Bidirectional Transfer Matrix for Detecting LSB Speech Steganography with Low Embedding Rates" (https://doi.org/10.1007/s11042-017-5505-0), co-authored by Wanxia Yang, Shanyu Tang, Miaoqi Li, Beibei Zhou, and Yijing Jiang, proposes a new steganalysis algorithm based on Markov bi-directional transition matrix (MBTM) of wavelet packet coefficient (WPC) of the second-order derivative-based speech signal. By using the MBTM feature, better expression for the correlation of WPC can be realized. A support vector machine (SVM) is used through training a large number of LSB hidden data with different embedding rates, which can effectively achieve the LSB matching steganalysis for speech signals. The proposed steganalysis algorithm has significant superiority compared with the classic methods based on histogram moment features, especially when the embedding rate is lower.

Another paper titled "Unsupervised Steganalysis over Social Networks Based on Multi-Reference Sub-image Sets" (https://doi.org/10.1007/s11042-017-4759-x), co-authored by Fengyong Li, Kui Wu, Jingsheng Lei, Mi Wen, and Yanli Ren, proposes a new unsupervised steganalysis scheme to identify individual JPEG image as stego or cover. This scheme doesn't require a great number of samples for training the classification model, which utilizes the calibration technique to construct multiple reference images based on one suspicious image. Through calculating the maximum mean discrepancy between two sub-image sets of suspicious image and reference images, an effective measure is applied to produce the optimal decision on the suspicious image. Evaluation results demonstrate that the proposed scheme outperforms some of state-of-the-art steganalysis schemes.

Currently, the studies of steganalysis mainly focus on the existence detection of hidden messages. But, the extraction of hidden messages, i.e., extraction attack, is also an important task for obtaining the evidence of covert communication. For the steganography using a stego key, the objective of an extraction attack is to recover the stego key. The paper titled "Stego Key Recovery Based on the Optimal Hypothesis Test" (https://doi.org/10.1007/s11042-017-4878-4), co-authored by Che Xu, Jiufen Liu, Junjun Gan, and Xiangyang Luo, studies methods of recovering the stego key for LSB steganography in JPEG domain based on the optimal hypothesis test model. According to the difference in coefficient distributions between the correct and erroneous paths, two methods for recovering the stego key of OutGuess and F5 steganography are proposed. Experimental results show that, the proposed methods can successfully recover the stego key for OutGuess 0.13b, OutGuess 0.2 and modified F5 steganography methods.

In the paper "Double-Compressed JPEG Images Steganalysis with Transferring Feature" (https://doi.org/10.1007/s11042-018-5734-x), Yong Yang, Xiangwei Kong, and Chaoyu Feng propose the transferring feature on double-compressed (TFD) JPEG images to improve steganalysis accuracy for detecting the presence of the hidden secret messages. The proposed scheme first detects the double-compressed images through constructing multi-classifier with Markov feature, and then the feature discrepancy between the training set and the testing set is minimized to generate a transformation matrix. Experimental results demonstrate that, the proposed scheme achieves better performance than some reported schemes of double-compressed mismatched steganalysis.

The well-known adaptive steganographic method, i.e., HUGO (Highly Undetectable steGO), has excellent anti-detection ability. Although existing steganalysis methods based on parameter recognition of STC can detect adaptive steganography when embedded message is in plaintext, the steganalysis methods are ineffective when embedded message is in ciphertext. The paper titled "Reliable Steganalysis of HUGO Steganography Based on

Partially Known Plaintext" (https://doi.org/10.1007/s11042-017-5134-7), co-authored by Junjun Gan, Jiufen Liu, Xiangyang Luo, Chunfang Yang, and Fenlin Liu, proposes a steganalysis algorithm based on partially known plaintext, in which the file format name and message length may be transmitted without encryption when HUGO steganography is applied to transmit the encrypted file. In this algorithm, the structural characteristics of the parity-check matrix are used to simplify the STC decoding. Experimental results demonstrate that, the parameter recognition of STC can be realized with an ordinary PC in a short time.

3 Reversible data hiding

The paper titled "A Novel Auxiliary Data Construction Scheme for Reversible Data Hiding in JPEG Images" (https://doi.org/10.1007/s11042-017-4557-5), co-authored by Jinpeng Lv, Sheng Li, and Xinpeng Zhang, presents a novel auxiliary data construction scheme for reversible data hiding (RDH) in JPEG images. The auxiliary data in this scheme is constructed by compressing the original LSBs conditioned on the reconstructed LSBs. Besides the auxiliary data construction, a coefficient selection strategy is also proposed in this paper to further improve compression rate. As a result, the size of auxiliary data in the proposed construction scheme is smaller than that directly compressed from the original LSBs. The proposed RDH scheme outperforms some of reported JPEG RDH schemes with file size preservation.

Another paper titled "A ROI-Based High Capacity Reversible Data Hiding Scheme with Contrast Enhancement for Medical Images" (https://doi.org/10.1007/s11042-017-4444-0), co-authored by Yang Yang, Weiming Zhang, Dong Liang, and Nenghai Yu, focuses on the secure archiving of medical images stored on semi-trusted cloud servers. The authors propose a novel region of interest (ROI) based high capacity RDH scheme with contrast enhancement, which can effectively improve the quality of medical images and reversibly embed high capacity data at the same time. The adaptive threshold detector (ATD) segmentation technique is first used in this paper to separate the ROI and the Non-ROI, and then the contrast of the ROI is enhanced by stretching the grayscale. The secret data can be successfully embedded into the peak bins of the stretched histogram without extending the histogram bins.

Recently, signal processing in encrypted domain (SPED) has attracted much attention because of the requirement of privacy preserving. The paper titled "Reversible Data Hiding in Encrypted AMBTC Images" (https://doi.org/10.1007/s11042-017-4957-6), co-authored by Zhaoxia Yin, Xuejing Niu, Xinpeng Zhang, Jin Tang, and Bin Luo, focuses on RDH in encrypted, compressed images. In the proposed scheme, the higher and the lower means of a triple in an AMBTC-compressed image are first encrypted with stream cipher, and the additional data are embedded into the redundant space through modifying the prediction error histogram. On the receiver side, the separable operations of data extraction, image decryption, and image recovery can be successfully achieved based on the availability of data hiding key and encryption key. In addition, the proposed scheme can be implemented with low computation complexity.

In the paper titled "Reversible Watermarking Based on Multi-Dimensional Prediction-Error Expansion", Xiang Yu, Xiang Wang, and Qingqi Pei extend the two-dimensional histogram shifting method and propose a reversible watermarking scheme based on multi-dimensional prediction-error expansion (PEE), which can reduce the distortion through abandoning the embedding mappings with high distortions and is more suitable to the images with the simple and smooth textures. The experimental results show that, the multi-dimensional PEE is superior to the two-dimensional PEE and achieves a better rate-distortion performance.

4 Cryptography

The paper titled "Verifiable Outsourced Attribute-Based Signature Scheme" (https://doi.org/10.1007/s11042-017-4539-7), co-authored by Yanli Ren and Tiejin Jiang, proposes a secure verifiable outsourced attribute-based signature (ABS) scheme, in which the computation overload of the signer can be outsourced to an untrusted signing-cloud service provider (S-CSP). Computation cost of the signer in the proposed scheme is greatly reduced, and the correctness of the output returned from the S-CSP can be verified through embedding some secret elements into the outsource keys and making them blind to the S-CSP. Experimental results show that, the computation cost for the signer is smaller than that of directly computing the signature, which can be applied for the resource-limited devices to realize the signing of an ABS system.

Deploying cryptographic algorithms within software applications, which are executed in untrusted environments owned and controlled by a possibly malicious party, is becoming increasingly common, and white-box cryptography aims to protect secret key in such an environment. But, AES was originally designed without considering the execution in a white-box attack context, which leads to the ease of breaking AES's white-box version due to the fixed confusion and diffusion operations. The paper titled "A White-Box AES-Like Implementation Based on Key-Dependent Substitution-Linear Transformations" (https://doi.org/10.1007/s11042-017-4562-8), co-authored by Tao Xu, Feng Liu, and Chuankun Wu, presents an AES-like cipher through substituting AES's S-boxes and MixColumn matrices with the key-dependent components and preserving their good cryptographic properties. Results show that, the white-box implementation of the proposed AES-like cipher can resist some of current known attacks.

5 Other emerging techniques

In the paper titled "Expose Noise Level Inconsistency Incorporating the Inhomogeneity Scoring Strategy" (https://doi.org/10.1007/s11042-017-5206-8), Heng Yao, Fang Cao, Zhenjun Tang, Jinwei Wang, and Tong Qiao focus on the problem that the estimation of the noise is inaccurate because of the complexity of the textures in the region. According to the scoring strategy-based, object-proposal technique, a new method incorporating the inhomogeneity scoring strategy is proposed in this paper, which provides a convincing result to expose image splicing operations. The noise variance of each image patch is calculated through pixel-level noise estimation method, and the most suspicious splicing region, i.e., the conjunct patches with the maximum area, can be identified by a linear equation fitting based on the estimated variance and inhomogeneity score.

Blind sharing of digital images by social networks is popular in recent years, which may also cause privacy threats. Only privacy decision recommendations and access control mechanism are not enough to solve this issue. The paper titled "How People Share Digital Images in Social Networks: A Questionnaire-Based Study of Privacy Decisions and Access Control" (https://doi.org/10.1007/s11042-017-4402-x), co-authored by Xiaoxia Hu, Donghui Hu, Shuli Zheng, Wangwang Li, Fan Chen, Zhaopin Shu, and Lina Wang, investigates the purposes, attitudes, preferences, modes and recommendations for sharing images based on the human-computer interaction. The survey concludes that, there is a partial order based on either the privacy level or attribute tag for image sharing, and it is important for current social networks to have fine-grained access control settings.

Fingerprint recognition is widely developed for authentication in many applications, which may be spoofed by artificial fingerprints generated with different materials. Therefore, the fingerprint liveness detection (FLD) is essential to judge whether a given fingerprint image is derived from a real finger or a spoofed one. In the paper titled "Rotation-invariant Weber Pattern and Gabor Feature for Fingerprint Liveness Detection" (https://doi.org/10.1007/s11042-017-5517-9), Zhihua Xia, Rui Lv, and Xingming Sun propose a feature extraction method for the FLD problem, which consists of two components, i.e., Weber local binary pattern (WLBP) and circularly symmetric Gabor feature (CSGF) for spatial domain and frequency domain, respectively. The final features are constructed with the co-occurrence probabilities of WLBP and CSGF. Experimental results conducted on two public databases show the effectiveness of the proposed method.

The publication of this special issue was achieved based on sincere cooperation. We wish to thank all the authors for the submission of their excellent works and also appreciate the technical reviewers and the Springer staffs for their hard and careful work. We do hope that the eighteen papers published in this special issue could make the reader of Multimedia Tools and Applications interested and rewarded. Specially, we would like to deeply thank Prof. Borko Furht, Editor-in-Chief of Multimedia Tools and Applications, for his great supports and helps from the beginning to the eventual publication of this special issue.

Chuan Qin received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently an Associate Professor. He was with Feng Chia University at Taiwan as a Postdoctoral Researcher and Adjunct Assistant Professor from July 2010 to July 2012. His research interests include image processing and multimedia security. He has published more than 90 papers in these research areas.

Weiming Zhang received his B.S. degree and PH.D. degree in 1999 and 2005 respectively from Information Engineering University, Zhengzhou, China. Currently, he is a full professor with the School of Information Science and Technology, University of Science and Technology of China. His research interests include information hiding, multimedia security, and privacy-preserving data searching and analysis. He has published more than 80 papers in journals and conferences including IEEE Trans. Information Theory, IEEE Trans. Image Processing, IEEE Trans. Inf. Foren. & Sec., and Information Hiding.

Xinpeng Zhang received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University. Now, he is a Professor of Fudan University. He was with the State University of New York at Binghamton as a visiting scholar from January 2010 to January 2011, and Konstanz University as an experienced researcher sponsored by the Alexander von Humboldt Foundation from March 2011 to May 2012. His research interests include multimedia security, image processing, and digital forensics. He has published more than 180 papers in these areas. Currently, he is an Associate Editor for the IEEE Transactions on Information Forensics and Security.